The Frobenius problem for Mersenne numerical semigroups

M.B. Branco

Setember 2014

This is joint work with: J.C. Rosales and D. Torrão

Introduction

• Marin Mersenne 1588-1648 was a French theologian, philosopher, mathematician and music theorist.

Introduction

• Marin Mersenne 1588-1648 was a French theologian, philosopher, mathematician and music theorist.

• Mersenne was in the center of the world of science and mathematics during the first half of the 1600.
He corresponded with his contemporaries the greatest scientists like Descartes, Galileo, Fermat, Pascal and Torricelli.

Introduction

• Marin Mersenne 1588-1648 was a French theologian, philosopher, mathematician and music theorist.

• Mersenne was in the center of the world of science and mathematics during the first half of the 1600.
He corresponded with his contemporaries the greatest scientists like Descartes, Galileo, Fermat, Pascal and Torricelli.

•A Mersenne number is a number of the form $x = 2^n - 1$ with $n \in \mathbb{N} \setminus \{0\}$.
The Mersenne numbers consist of copies of the single digit 1 in base-2 and are therefore binary repunits.

Introduction

• Marin Mersenne 1588-1648 was a French theologian, philosopher, mathematician and music theorist.

• Mersenne was in the center of the world of science and mathematics during the first half of the 1600.
He corresponded with his contemporaries the greatest scientists like Descartes, Galileo, Fermat, Pascal and Torricelli.

• A Mersenne number is a number of the form $x = 2^n - 1$ with $n \in \mathbb{N} \backslash \{0\}$.
The Mersenne numbers consist of copies of the single digit 1 in base-2 and are therefore binary repunits.

• Mersenne is remembered today thanks to his association with the Mersenne primes which have been studied because of the remarkable property: every Mersenne prime corresponds to exactly one perfect number.
He compiled a list of Mersenne primes with exponents up to 257.

- A numerical semigroup S is a submonoid of $\mathbb{N}$ such that $\gcd(S) = 1$.

- A numerical semigroup S is a submonoid of $\mathbb{N}$ such that $\gcd(S) = 1$.
- S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$,

• A numerical semigroup S is a submonoid of $\mathbb{N}$ such that gcd $(S) = 1$.

• S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$, and the cardinality of its minimal system of generators is the embedding dimension of S, denoted by $e(S) = p$.

• A numerical semigroup S is a submonoid of $\mathbb{N}$ such that gcd $(S) = 1$.

• S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$, and the cardinality of its minimal system of generators is the embedding dimension of S, denoted by $\mathrm{e}(S) = p$.

• $\mathbb{N} \backslash S$ has finitely many elements and its cardinality is the genus of S, denoted by $\mathrm{g}(S)$.

• A numerical semigroup S is a submonoid of $\mathbb{N}$ such that $\gcd(S) = 1$.

• S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$, and the cardinality of its minimal system of generators is the embedding dimension of S, denoted by $e(S) = p$.

• $\mathbb{N} \backslash S$ has finitely many elements and its cardinality is the genus of S, denoted by $g(S)$.

• The greatest integer not in S is the Frobenius number, denoted by $F(S)$.

- A numerical semigroup S is a submonoid of $\mathbb{N}$ such that gcd $(S) = 1$.

- S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$, and the cardinality of its minimal system of generators is the embedding dimension of S, denoted by $\mathrm{e}(S) = p$.

- $\mathbb{N} \backslash S$ has finitely many elements and its cardinality is the genus of S, denoted by $\mathrm{g}(S)$.

- The greatest integer not in S is the Frobenius number, denoted by $\mathrm{F}(S)$.

- $x \in \mathbb{Z} \setminus S$ is a pseudo-Frobenius number of S if $x + (S \setminus \{0\}) \subseteq S$, the set of pseudo-Frobenius numbers of S is denoted by $Pg(S)$ and #Pg(s)= type(S).

- A numerical semigroup S is a submonoid of $\mathbb{N}$ such that gcd $(S) = 1$.

- S has a unique minimal system of generators $S = \langle n_1, \cdots, n_p \rangle$, and the cardinality of its minimal system of generators is the embedding dimension of S, denoted by $\mathrm{e}(S) = p$.

- $\mathbb{N} \backslash S$ has finitely many elements and its cardinality is the genus of S, denoted by $\mathrm{g}(S)$.

- The greatest integer not in S is the Frobenius number, denoted by $\mathrm{F}(S)$.

- $x \in \mathbb{Z} \setminus S$ is a pseudo-Frobenius number of S if $x + (S \setminus \{0\}) \subseteq S$, the set of pseudo-Frobenius numbers of S is denoted by $Pg(S)$ and #Pg(s)= type(S).

- A numerical semigroup is a Mersenne numerical semigroup if there exist $n \in \mathbb{N} \backslash \{0\}$ such that $S(n) = \left\langle \left\{ 2^{n+i} - 1 \mid i \in \mathbb{N} \right\} \right\rangle$.

- The Frobenius problem consists in finding a formula for computing $\mathrm{F}(S)$ and $\mathrm{g}(S)$ in terms of the elements in a minimal system of generators of S.

The problem

The Frobenius problem

- The Frobenius problem consists in finding a formula for computing $\mathrm{F}(S)$ and $\mathrm{g}(S)$ in terms of the elements in a minimal system of generators of S.
- The Frobenius problem was solved by Sylvester for numerical semigroups with $\mathrm{e}(S) = 2$.

- The Frobenius problem consists in finding a formula for computing $\mathrm{F}(S)$ and $\mathrm{g}(S)$ in terms of the elements in a minimal system of generators of S.
- The Frobenius problem was solved by Sylvester for numerical semigroups with $\mathrm{e}(S) = 2$.
- This problem remains open for numerical semigroups with $\mathrm{e}(S) \geq 3$.

The problem

The Frobenius problem

• The Frobenius problem consists in finding a formula for computing $\mathrm{F}(S)$ and $\mathrm{g}(S)$ in terms of the elements in a minimal system of generators of S.

• The Frobenius problem was solved by Sylvester for numerical semigroups with $\mathrm{e}(S) = 2$.

• This problem remains open for numerical semigroups with $\mathrm{e}(S) \geq 3$.

• In this work, we give formulas for the embedding dimension, the Frobenius number, the type and the genus for a Mersenne numerical semigroup.

The embedding dimension

The next result is the key to the development of this section.

The next result is the key to the development of this section.

Proposition

If n is a positive integer, then $S(n)$ is a numerical semigroup. Furthermore, $2s+1 \in S(n)$ for all $s \in S(n)\backslash\{0\}$.

The next result is the key to the development of this section.

Proposition

If n is a positive integer, then $S(n)$ is a numerical semigroup. Furthermore, $2s+1 \in S(n)$ for all $s \in S(n)\backslash\{0\}$.

Theorem

Let n be a positive integer and let $S(n)$ be the Mersenne numerical semigroup associated to n, then $e(S(n)) = n$. Furthermore $\left\{2^{n+i}-1 \mid i \in \{0,1,\ldots,n-1\}\right\}$ is the minimal system of generators of $S(n)$.

The Apéry set

For $n \in S \setminus \{0\}$ we define $\mathrm{Ap}(S, n) = \{s \in S : \ s - n \notin S\}$
It is easy to prove

For $n \in S \setminus \{0\}$ we define $\mathrm{Ap}(S,n) = \{s \in S : \; s - n \notin S\}$
It is easy to prove

Lemma

If $n \in S \setminus \{0\}$, then $\mathrm{Ap}(S,n) = \{w(0), \ldots, w(n-1)\}$ where $w(i) = \min\{s \in S \mid s \equiv i \bmod n \; (\forall i \in \{0, \ldots, n-1\})$.

For $n \in S \setminus \{0\}$ we define $\mathrm{Ap}(S,n) = \{s \in S : \ s - n \notin S\}$
It is easy to prove

Lemma

If $n \in S \setminus \{0\}$, then $\mathrm{Ap}(S,n) = \{w(0), \ldots, w(n-1)\}$ where $w(i) = \min\{s \in S \mid s \equiv i \bmod n \ (\forall i \in \{0, \ldots, n-1\})$.

The next, is due to Selmer, can be used to compute $\mathrm{F}(S)$ and $\mathrm{g}(S)$, from one of the Apery sets

For $n \in S \setminus \{0\}$ we define $\mathrm{Ap}(S, n) = \{s \in S : \ s - n \notin S\}$
It is easy to prove

Lemma

If $n \in S \setminus \{0\}$, then $\mathrm{Ap}(S, n) = \{w(0), \ldots, w(n-1)\}$ where $w(i) = \min\{s \in S \mid s \equiv i \bmod n \ (\forall i \in \{0, \ldots, n-1\})$.

The next, is due to Selmer, can be used to compute $\mathrm{F}(S)$ and $\mathrm{g}(S)$, from one of the Apery sets

Lemma

Let S be a numerical semigroup and let $x \in S \setminus \{0\}$. Then:

1) $\mathrm{F}(S) = \max\left(\mathrm{Ap}(S, x)\right) - x$;
2) $\mathrm{g}(S) = \frac{1}{x}\left(\sum_{w \in \mathrm{Ap}(S,x)} w\right) - \frac{x-1}{2}$.

For $n \in S \setminus \{0\}$ we define $\mathrm{Ap}(S,n) = \{s \in S : \ s - n \notin S\}$
It is easy to prove

Lemma

If $n \in S \setminus \{0\}$, then $\mathrm{Ap}(S,n) = \{w(0), \ldots, w(n-1)\}$ where $w(i) = \min\{s \in S \mid s \equiv i \mod n \ (\forall i \in \{0, \ldots, n-1\})$.

The next, is due to Selmer, can be used to compute $\mathrm{F}(S)$ and $\mathrm{g}(S)$, from one of the Apery sets

Lemma

Let S be a numerical semigroup and let $x \in S \setminus \{0\}$. Then:

1) $\mathrm{F}(S) = \max\left(\mathrm{Ap}(S,x)\right) - x$;
2) $\mathrm{g}(S) = \frac{1}{x}\left(\sum_{w \in \mathrm{Ap}(S,x)} w\right) - \frac{x-1}{2}$.

From now on we will denote by s_i the elements $2^{n+i} - 1$ for each $i \in \{0, 1, \ldots, n-1\}$

We say that a sequence $(a_1, \dots, a_k)$ is a residual k-tuple if satisfies the following conditions:

1. for every $i \in \{1, \dots, k\}$ we have that $a_i \in \{0, 1, 2\}$;
2. if $i \in \{2, \dots, k\}$ and $a_i = 2$ then $a_1 = \cdots = a_{i-1} = 0$.

We say that a sequence $(a_1, \ldots, a_k)$ is a residual k-tuple if satisfies the following conditions:

1. for every $i \in \{1, \ldots, k\}$ we have that $a_i \in \{0, 1, 2\}$;
2. if $i \in \{2, \ldots, k\}$ and $a_i = 2$ then $a_1 = \cdots = a_{i-1} = 0$.

Theorem

Let n be an integer greater than or equal to two and let $S(n)$ be the Mersenne numerical semigroup minimally generated by $\{s_0, s_1, \ldots, s_{n-1}\}$. Then
$\mathrm{Ap}\,(S(n), s_0) =$
$\{a_1 s_1 + \cdots + a_{n-1} s_{n-1} \mid (a_1, \ldots, a_{n-1}) \text{ is a residual } (n-1)-\text{tuple}\}$.

We say that a sequence $(a_1, \ldots, a_k)$ is a residual k-tuple if satisfies the following conditions:

1. for every $i \in \{1, \ldots, k\}$ we have that $a_i \in \{0, 1, 2\}$;
2. if $i \in \{2, \ldots, k\}$ and $a_i = 2$ then $a_1 = \cdots = a_{i-1} = 0$.

Theorem

Let n be an integer greater than or equal to two and let $S(n)$ be the Mersenne numerical semigroup minimally generated by $\{s_0, s_1, \ldots, s_{n-1}\}$. Then
$\mathrm{Ap}\,(S(n), s_0) =$
$\{a_1 s_1 + \cdots + a_{n-1} s_{n-1} \mid (a_1, \ldots, a_{n-1}) \text{ is a residual } (n-1)-\text{tuple}\}$.

Example

Let us compute $\mathrm{Ap}\,(S(4), s_0)$. We have that $s_0 = 15$ and $S(4) = \langle\{15, 31, 63, 127\}\rangle$. The residual 3-tuples are $(0,0,0)$, $(0,1,0)$, $(0,0,1)$, $(0,1,1)$, $(1,0,0)$, $(1,1,0)$, $(1,0,1)$, $(1,1,1)$, $(2,0,0)$, $(2,1,0)$, $(2,0,1)$, $(2,1,1)$, $(0,2,0)$, $(0,2,1)$ and $(0,0,2)$. Since $s_1 = 31$ $s_2 = 63$ and $s_3 = 127$, by previous theorem we obtain that $\mathrm{Ap}\,(S(4), s_0) =$
$\{0, 63, 127, 190, 31, 94, 158, 221, 62, 125, 189, 252, 126, 253, 254\}$.

The Frobenius problem

Now we give a formula for the greatest integer that does not belong to $S(n)$. Let us denote by R the set of all residual $(n-1)$-tuples.

Now we give a formula for the greatest integer that does not belong to $S(n)$. Let us denote by R the set of all residual $(n-1)$-tuples.

Lemma

Let n be an integer greater than or equal to two and let R be the set of all residual $(n-1)$*-tuples. Then the maximal elements (with respect to the product order) in R are* $(2, 1, \ldots, 1)$, $(0, 2, 1, \ldots, 1)$ *and* $(0, 0, \ldots, 2)$.

Now we give a formula for the greatest integer that does not belong to $S(n)$. Let us denote by R the set of all residual $(n-1)$-tuples.

Lemma

Let n be an integer greater than or equal to two and let R be the set of all residual $(n-1)$-tuples. Then the maximal elements (with respect to the product order) in R are $(2,1,\ldots,1)$, $(0,2,1,\ldots,1)$ and $(0,0,\ldots,2)$.

We will prove that $2s_1+s_2+\cdots+s_{n-1}, 2s_2+s_3+\cdots+s_{n-1}, \ldots, 2s_{n-1}$ is a sequence of integers wherein each term is obtained from the previous by adding a unit.

Now we give a formula for the greatest integer that does not belong to $S(n)$. Let us denote by R the set of all residual $(n-1)$-tuples.

Lemma

Let n be an integer greater than or equal to two and let R be the set of all residual $(n-1)$*-tuples. Then the maximal elements (with respect to the product order) in R are* $(2, 1, \ldots, 1)$, $(0, 2, 1, \ldots, 1)$ *and* $(0, 0, \ldots, 2)$.

We will prove that $2s_1 + s_2 + \cdots + s_{n-1}, 2s_2 + s_3 + \cdots + s_{n-1}, \ldots, 2s_{n-1}$ is a sequence of integers wherein each term is obtained from the previous by adding a unit.

Thus we give the a formula for the Frobenius number of a Mersenne numerical semigroup.

Theorem

Let n be an integer greater than or equal to two and let $S(n)$ *be the Mersenne numerical semigroup associated to n. Then* $\mathrm{F}(S(n)) = 2^{2n} - 2^n - 1$.

We can define in $\mathbb{Z}$ the following order relation: $a \leq_S b$ if $b - a \in S$

We can define in $\mathbb{Z}$ the following order relation: $a \leq_S b$ if $b - a \in S$
The following result gives a formula for the pseudo-Frobenius numbers in terms of the Apéry sets.

We can define in $\mathbb{Z}$ the following order relation: $a \leq_S b$ if $b - a \in S$
The following result gives a formula for the pseudo-Frobenius numbers in terms of the Apéry sets.

Lemma

Let S be a numerical semigroup and $x \in S \setminus \{0\}$. Then

$$\mathrm{PF}(S) = \{w - x \mid w \in \mathrm{Maximales}_{\leq_S} \mathrm{Ap}(S, x)\}$$

We can define in $\mathbb{Z}$ the following order relation: $a \leq_S b$ if $b - a \in S$
The following result gives a formula for the pseudo-Frobenius numbers in terms of the Apéry sets.

Lemma

Let S be a numerical semigroup and $x \in S \setminus \{0\}$. Then

$$\mathrm{PF}(S) = \{w - x \mid w \in \mathrm{Maximales}_{\leq_S} \mathrm{Ap}(S, x)\}$$

Theorem

Let n be an integer greater than or equal to two and let $S(n)$ be the Mersenne numerical semigroup associated to n. Then type$(S(n)) = n - 1$. Furthermore

$$\mathrm{PF}\left(S(n)\right) = \left\{\mathrm{F}\left(S(n)\right), \mathrm{F}\left(S(n)\right) - 1, \ldots, \mathrm{F}\left(S(n)\right) - (n-2)\right\}.$$

The next result gives the formula for the gender of the Mersenne numerical semigroup $S(n)$.

The next result gives the formula for the gender of the Mersenne numerical semigroup $S(n)$.

Theorem

Let n be a positive integer and let $S(n)$ be the Mersenne numerical semigroup associated to n. Then $\mathrm{g}(S(n)) = 2^{n-1}(2^n + n - 3)$.

The next result gives the formula for the gender of the Mersenne numerical semigroup $S(n)$.

Theorem

Let n be a positive integer and let $S(n)$ be the Mersenne numerical semigroup associated to n. Then $\mathrm{g}\left(S(n)\right) = 2^{n-1}\left(2^n + n - 3\right)$.

Example

Let us compute the the Frobenius number, the type and gender of the Mersenne numerical semigroup $S(4)$. By using previous results we obtain that $\mathrm{F}\left(S(4)\right) = 2^8 - 2^4 - 1 = 239$. We have that $\mathrm{type}(S(4)) = 3$ and $\mathrm{PF}\left(S(4)\right) = \{239, 238, 237\}$. Finally, we get that $\mathrm{g}\left(S(4)\right) = 2^3\left(2^4 + 4 - 3\right) = 136$.